Strategy Research Project

# EMERGENCY RESPONSE: UNITY OF EFFORT THROUGH A COMMON OPERATIONAL PICTURE

BY

LIEUTENANT COLONEL JEFFREY COPELAND
United States Army National Guard



USAWC CLASS OF 2008



U.S. Army War College, Carlisle Barracks, PA 17013-5050

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **15 MAR 2008** | **Strategy Research Project** | **00-00-2007 to 00-00-2008** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Emergency Response: Unity of Effort Through a Common Operational Picture** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| **Jeffrey Copeland** | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| **U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220** | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**See attached**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **32** | |

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

# EMERGENCY RESPONSE: UNITY OF EFFORT THROUGH A COMMON OPERATIONAL PICTURE

by

Lieutenant Colonel Jeffrey Copeland
United States Army National Guard

Mr. William Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Lieutenant Colonel Jeffrey Copeland

TITLE: Emergency Response: Unity of Effort through a Common Operational Picture

FORMAT: Strategy Research Project

DATE: 25 March 2008 WORD COUNT: 5,922 PAGES: 31

KEY TERMS: DHS, Incidents of National Significance, Homeland Security

CLASSIFICATION: Unclassified

This research paper will review current operational constructs in emergency response specifically focusing on incidents of national significance where multiple organizations must manage crisis, respond, and provide services as an integrated team. These organizations primarily include, but are not limited to, the Department of Homeland Security, the military – both active and reserve components, and civil authorities including first responders. With a focus on improving unity of effort, the common operational picture will be explored as a means to support decision making, coordination, and integration between emergency response organizations. With a common framework for collecting and disseminating information, agencies can improve efficiency, make better use of resources, and provide a coordinated and timely response during crisis. The goal is to review the roles, responsibilities, and capabilities of emergency response organizations and identify the requirements, opportunities, and challenges in the design and implementation of a common operational picture.

# EMERGENCY RESPONSE: UNITY OF EFFORT THROUGH A COMMON OPERATIONAL PICTURE

This research paper will review current operational constructs in emergency response specifically focusing on incidents of national significance where multiple organizations must manage crisis, respond, and provide services as an integrated team. These organizations primarily include, but are not limited to, the Department of Homeland Security, the military – both active and reserve components, and civil authorities including first responders. With a focus on improving unity of effort, the common operational picture will be explored as a means to support decision making, coordination, and integration between emergency response organizations.

With a common framework for collecting and disseminating information, agencies can improve efficiency, make better use of resources, and provide a coordinated and timely response during crisis. The goal is to review the roles, responsibilities, and capabilities of emergency response organizations and identify the requirements, opportunities, and challenges in the design and implementation of a common operational picture (COP).

## Background

Hurricane Katrina serves as a prime example of an incident of national significance where emergency response requirements quickly exceeded the capability of local and state agencies. With multiple states affected and federal assistance requested, organizations from around the country and the world were poised and ready to assist. The challenge was the lack of situational awareness and the means to provide a coordinated and efficient response by local, state, and federal agencies.

## Defining Common Operational Picture

Emergency response agencies do not share a common understanding and definition of a common operational picture. There are disagreements as to whether a common operational picture is a product, process, or operating environment. This lack of understanding and agreement has led to many organizations creating “stove pipe” systems that are not interconnected and not capable of sharing critical information needed across agencies in order to effectively manage a crisis once requirements have overwhelmed state, local, and private sector agencies.

The National Response Plan (NRP) establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. It forms the basis of how the federal government coordinates with state, local, and tribal governments and the private sector during incidents. The NRP defines common operational picture as a broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence.[1] The NRP directs the use of the National Incident Management System (NIMS) which provides this more detailed description: “A common operating picture is established and maintained by the gathering, collating, synthesizing, and disseminating of incident information to all appropriate parties involved in an incident. Achieving a common operating picture allows on−scene and off−scene personnel to have the same information about the incident, including the availability and location of resources, personnel, and the status of requests for assistance. Additionally, a common operating picture offers an overview of an incident thereby providing incident information which enables the Incident Commander (IC), Unified Command (UC), and supporting agencies and organizations

to make effective, consistent, and timely decisions. In order to maintain situational awareness, communications and incident information must be updated continually."[2]

The Department of Defense defines common operational picture as "a single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness."[3] Chairman of the Joint Chiefs of Staff Instruction 3151.01A which pertains to the Global Command and Control System COP Reporting Requirements defines common operational picture as: "a distributed data processing and exchange environment for developing a dynamic database of objects, allowing each user to filter and contribute to this database, according to the user's area of responsibility and command role. The common operational picture provides the integrated capability to receive, correlate, and display a common tactical picture, including planning applications and theater-generated overlays and projections (i.e., environmental, battle plans, force position projections)."[4]

In July of 2007 the United States Army War College's Center for Strategic Leadership hosted The Sixth Annual USAWC Reserve Component Symposium Achieving Unity of Effort in Responding to Crisis. One of four workshops, entitled "Development and Dissemination of a 'Common Operational Picture' in Preparation, Response, and Recovery Operations between the Components of the Military and Civilian Authorities at All Levels of Government" explored the definition of a "Common Operational Picture." Symposium participants represented a broad spectrum of leading stakeholders including the Office of the Assistant Secretary of Defense for Homeland Defense and Americas Security Affairs, the Department of Homeland Security, United

States Northern Command, National Guard Bureau, Office of the Chief of Army Reserve Affairs, and the Adjutants General the states of Georgia, Rhode Island, and Texas, the Pennsylvania  Director of Homeland Security, and multiple representatives of both the public and private sector.

Workshop participants broke down each term independently and provided insights. With respect to “Common,” potential users of the COP include every level of leadership from local first responders thru community, state, regional and federal level. The inability to realistically expect that a single COP would actually suit this broad audience drove many to argue that a common database is more likely to be useful than any particular common depiction.”[5] With respect to “Operational,” the COP needs to be more than a handy geospatial picture. The COP must depict not only what is ongoing currently but also depict those things that facilitate situational awareness over a longer term (readiness, logistics, future availabilities, etc.) with agreement that the correct term to use is “operational” as opposed to “operating.”[6] With respect to “Picture,” no single proposed COP entity was perceived as the “best” answer although there were common elements identified for each type of crisis. The group determined that a COP can best be developed by creating accepted standards for inputs and outputs and providing analytical support that is readily accessible, rather than dictating the “picture content.”[7]

Mandates for Responding to Incidents of National Significance

In response to the attacks of 11 September 2001, President George W. Bush worked with Congress to enact the Homeland Security Act of 2002 which created the Department of Homeland Security (DHS). Homeland Security Presidential Directive 5 (HSPD-5), titled Management of Domestic Incidents was issued on 28 February 2003.

HSPD-5 identified the objective of ensuring "all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management."[8] HSPD-5 directed the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). The NIMS would "provide a consistent nationwide approach for federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of the cause, size, or complexity."[9] HSPD-5 also tasked the Secretary of Homeland Security to establish a National Response Plan to integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan."[10]

The Department of Homeland Security published the National Response Plan in December 2004. The NRP included a letter of agreement signed by a number of federal agencies including Departments of Homeland Security, Defense, Energy, Health and Human Services, Interior, Labor, Transportation, and Treasury, as well as others. The NRP is based on three planning assumptions. First, "incidents are typically managed at the lowest possible geographic, organizational, and jurisdictional level."[11] Second, "the combined expertise and capabilities of the government at all levels, the private sector, and nongovernmental organizations will be required to prevent, prepare for, respond to, and recover from incidents of national significance.[12] Third, an incident of national significance may "overwhelm capabilities of State, local, and tribal governments, and private-sector infrastructure owners and operators."[13]

The NRP defines an incident of national significance (INS) as "an actual or potential high-impact event that requires robust coordination of the Federal response in

order to save lives and minimize damage, and provides the basis for long-term community and economic recovery. The Secretary of Homeland Security, in consultation with other departments and agencies, and the White House, as appropriate, declares INS."[14] "For INS that are Presidentially declared disasters or emergencies, Federal support to States is delivered in accordance with relevant provisions of the Stafford Act."[15] "The Secretary of Homeland Security will manage the Federal Government's response following the declaration of an INS."[16]

Under provisions of the Stafford Act and applicable regulations, a governor may request the President to declare a major disaster or emergency if the governor finds that effective response to the event is beyond the combined response capabilities of the State and affected local governments.[17]

## Analysis

### Emergency Response Players

The Department of Homeland Security is identified as the over-arching authority at the federal level for coordinating response to incidents of national significance. In compliance with presidential directives, DHS has provided a framework and guidelines for emergency response coordination at all levels including federal, state, local, and private organizations and agencies. This framework emanates from the National Response Plan, National Preparedness Goal, National Incident Management System, and the Incident Command System.

The Department of Defense is committed to supporting the National Response Plan as evidenced by a Deputy Secretary of Defense memorandum dated 29 November 2005 that directs department wide compliance with NIMS.

United States Northern Command (USNORTHCOM) mission is to anticipate and conduct Homeland Defense and Civil Support operations within the assigned area of responsibility to defend, protect, and secure the United States and its interests. USNORTHCOM plans, organizes, and executes homeland defense and civil support missions, but has few permanently assigned forces. The command is assigned forces whenever necessary to execute missions, as ordered by the President and Secretary of Defense. USNORTHCOM's civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes.

An emergency must exceed the capabilities of local, state and federal agencies before USNORTHCOM becomes involved. In most cases, support will be limited, localized and specific. When the scope of the disaster is reduced to the point that the Lead Agency can again assume full control and management without military assistance, USNORTHCOM will exit, leaving the on-scene experts to finish the job.[18] General Renuart, the current NORTHCOM Commander explains his organization's role as "our job is not to come in and take over an operation in a state. Our job is to ensure that as the Governor and the adjutant general see the need, we are on the doorstep with the right kinds of capabilities for them to continue their response, or to increase the size of their response, or to sustain it over time in an area where it might be a long recovery process."[19]

The National Guard is postured, as a home town entity in more than 2700 local communities to provide a key advantage to both the federal government and state governors for responding effectively to domestic emergencies. The National Guard is equipped to respond quickly and on short notice.

The emergency response community reminds us that all disasters are “local.” That axiom has led to a universal recognition of the National Guard as the military’s force of choice in responding to domestic disasters. As a part if the community themselves, they possess an understanding, a familiarity, and a relationship with state and local authorities that the active component of the military could never hope to replicate. By extension, in dealing with state and local authorities which transcend the borders and capacities of a state, a cooperative effort led by the National Guard in providing for a regional response may fill a critical gap in saving and sustaining life.[20]

The National Guard Bureau (NGB) functions as a focal point and channel of communications among the Departments of the Army (DA) and Air Force (DAF), the states, and the National Guard. NGB is a joint bureau of the DA and the DAF, serving both as a staff and an operating agency. NGB is mandated to monitor and assist “the States in the organization, maintenance, and operation of National Guard units ensuring they can fulfill their federal and state missions. The governor of a state is the commander-in-chief of the National Guard unless mobilized for federal service by the president of the United States.”

Each state government has an Emergency Services Office or equivalent organization that coordinates resources and emergency response operations. Each state’s emergency response organization and structure differs based on the individual state’s requirements and capabilities. These state offices are linked to the Federal Emergency Management Agency (FEMA). Federal support must be requested by the state and is normally provided through FEMA if approved. Each state also has a Department of Homeland Security Director.

## Current Emergency Response Information Sharing Capabilities

The Homeland Security Information Network (HSIN) is a secure, unclassified, web-based communications system that serves as DHS's primary nation-wide information sharing and collaboration network. HSIN offers real-time chat and instant messaging capability, as well as a document library that contains reports from multiple federal, state, and local sources. HSIN supplies suspicious incident and pre-incident information, mapping and imagery tools, 24x7 situational awareness, and analysis of terrorist threats, tactics, and weapons. The network provides connectivity between DHS's Homeland Security Operations Center (HSOC), critical private industry, federal, state, and local organizations responsible for or involved in combating terrorism, responding to critical incidents, and managing special events. The HSOC, which provides oversight responsibility for HSIN, is the primary national-level center for real-time threat monitoring, domestic incident management, and information sharing.[21]

Across the various levels of government, a number of communities share information through the HSIN, including law enforcement, emergency management, fire departments, homeland security, counter-terrorism, and the National Guard.

The Department of Homeland Security Inspector General published a report titled "Homeland Security Information Network Could Support Information Sharing More Effectively" in June 2006. The report found that due to time pressures, DHS did not complete a number of the steps essential to effective system planning and implementation, hindering the success of the HSIN system. Specifically, DHS did not clearly define HSIN's relationship to existing collaboration systems and also did not obtain and address requirements from all HSIN user communities in developing the system. In addition, DHS did not adequately evaluate each of its three major HSIN

releases prior to their implementation. Further, the department has not provided adequate user guidance, including clear information sharing processes, training, and reference materials. Without establishing a baseline and developing specific performance measures, DHS has no effective way to track or assess information sharing using HSIN. As a result of these system planning and implementation issues, HSIN is not effectively supporting state and local information sharing. Although users generally like the web portal technology because of its user-friendliness and flexibility, those we interviewed said they are not committed to the system approach. Users are confused and frustrated, without clear guidance on HSIN's role or how to use the system to share information effectively. Because some lack trust in the system's ability to safeguard sensitive information, and because the system does not provide them with useful situational awareness and classified information, users do not regularly use HSIN. Instead, users resort to pre-existing means such as related systems and telephone calls to share information, which only perpetuates the ad hoc, stove-piped information-sharing environment that HSIN was intended to correct. Resources, legislative constraints, privacy, and cultural challenges–often beyond the control of HSIN program management–also pose obstacles to HSIN's success.[22]

USNORTHCOM utilizes a number of different systems that comprise their Common Operational Picture both in an unclassified and classified format. These systems, both commercial products and in-house applications, include Situational Awareness Geospatial Enterprise (SAGE), Global Command and Control System (GCCS), Command and Control Personal Computer (C2PC), and TRITON. According to a briefing presented by COL Robert Felderman, Deputy Director of Operations for

Land and National Guard Matters DJ3-NG, the USNORTHCOM COP maintains a COP to fuse, analyze and assess information required to create and share situational awareness. Inputs to the COP supporting homeland defense and civil support are inherent to the missions of Joint Forces Land (JFLCC), Air (JFACC) and Maritime Component Commanders (JFMCC), plus assigned Joint Task Forces (JTFs) that fall within the USNORTHCOM organization. The USNORTHCOM COP requires understanding of friendly and threat environmental information. Reporting of quality information requires timeliness, accuracy, relevance, usefulness, completeness, conciseness, security, understandability, and simplicity.

The National Guard Bureau contracted with commercial partners to build a proprietary system called the Joint Information Exchange Enterprise (JIEE) to serve as the National Guard Bureau's COP. JIEE is an information collection, collation, organization, dissemination and archival tool, providing real-time Situational Awareness (SA) and an automated, shared operational picture. JIEE provides the National Guard Bureau's Joint Operations Center (JOC) staff with a 'desktop' to share event and crisis management information as well as a clear operational picture enabling senior leadership to make rapid, accurate, and fully informed decisions. JIEE also supports content and document management tasks while providing data mining, data visualization, and operations tracking tools. The NGB Joint Operations Center utilizes JIEE to track requests for information (RFI), organize responses and coordinate support to assist first-responders, share information among the state guard units and to keep leadership fully aware of events and decision requirements. Information 'pull' and selective information 'push' features activated at the operations center level, enable

those closest to the situation to gather and disseminate cogent information to those requiring it, without overloading others.[23]

Each state National Guard has a Joint Force Headquarters (JFHQ) to provide command and control of all National Guard forces in the state or territory for the governor. The JFHQ supports JTF-State commanders and all of the deployed units within the state, as well as acting as an information channel to the National Guard Bureau. The JFHQ-State coordinates any additional support required, such as mobilization of extra forces, or providing other logistical support. National Guard Bureau directs that each state National Guard input information into the JIEE system. Each state National Guard also serves under the control of the governor and interfaces with state government emergency management authorities.

State emergency management agencies utilize various systems to provide a COP with no standardization among states other than the NIMS compatibility requirements which are generic in nature. According to a recent survey conducted by National Guard Bureau, the most prevalent application being utilized among state emergency management agencies, in conjunction with state National Guard organizations, is the WebEOC® commercial product provided by ESI Incorporated.

Many challenges exist in establishing a common operational picture by emergency response entities. Smaller first responder organizations face different challenges than larger agencies. Local organizations generally have fewer resources and less incentive to establish a common operational picture for use beyond their immediate organization as the majority of incidents are smaller scale requiring fewer resources and can be managed without the need for outside assistance. Larger

organizations have more resources with significant incentives to establish a common operational picture but must deal with a larger diverse group of agencies with established systems and processes with a prevailing culture that is not willing to embrace needed change when they can meet their local needs with local proprietary systems. These proprietary systems along with lack of integrated exercises among the different agencies provide for an emergency response effort that is many times uncoordinated and inefficient.

Incidents of national significance requiring support beyond the state level often involve agencies that do not use interoperable systems with standards permitting the sharing, access, and manipulation of data to provide situational awareness. Differing jurisdictions, regulations, and operating procedures normally preclude unity of command and the lack of established standards for sharing data and proprietary systems make unity of effort challenging in providing an effective emergency response.

Unified Approach

*Unity of Command* means that each individual participating in the operation reports to only one supervisor. This eliminates the potential for individuals to receive conflicting orders from a variety of supervisors, thus increasing accountability, preventing freelancing, improving the flow of information, helping with the coordination of operational efforts, and enhancing operational safety.[24]

The tiered response framework for domestic emergency response works well at the local and state level where first responders can anticipate requirements, react quickly, coordinate necessary actions, and make decisions in a crisis management situation. Local and state response agencies are normally familiar with their operating

area. Responders have often planned and participated in exercises working as an integrated team where unity of command is established in a pre-determined and clear hierarchy where there is no question about authority or who is “in charge.”

The DOD dictionary defines *unity of effort* as coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization - the product of successful unified action.

Unity of command can become a major issue when both federal and state militaries simultaneously provide Defense Support to Civil Authorities (DSCA) within the same area of operations. Both federal and state militaries look alike and have similar equipment, but are commanded by different authorities. Federal and state laws and policies regulate the missions each may perform based on the activated status (Title 10, Title 32, or State Active Duty).

The 2006 Quadrennial Defense Review calls for increasing unity of effort to achieve the nation’s security policy priorities across the agencies of the Federal Government. To address the many security challenges more effectively, the Department of Defense is continuing to shift its emphasis from department-centric approaches toward interagency solutions. Cooperation across the Federal Government begins in the field with the development of shared perspectives and achieving unity of effort and a better understanding of each agency’s role, missions and capabilities. This will complement better understanding and closer cooperation in Washington, and will extend to execution of complex operations.[25]

Preparedness requires a unified approach to emergency management and incident response activities. To achieve this, components of NIMS must be woven

together within a jurisdiction's or organization's emergency management and incident response structure. Preparedness must be integrated into management of communications, information, resources, and command to form an effective system. These characteristics allow organizations with different jurisdictional, geographical, and/or functional responsibilities, authorities, and resources to coordinate, plan, and interact effectively in support of a commonly recognized objective.[26]

NIMS provides a structured approach to operations allowing multiple organizations to work together in situations where unity of command is not feasible and success depends on coordination, collaboration and unity of effort.

Command Functions

The National Incident Management System describes two command functions: Single Command Incident Command and Unified Command. Single Command Incident Command occurs within a single jurisdiction where there is no jurisdictional or functional agency overlap. A single IC should be designated with overall incident management responsibility by the appropriate jurisdictional authority. ICs should be pre-designated in preparedness plans if possible. The designated IC will develop the incident objectives on which subsequent incident action planning will be based.[27] These single jurisdiction or single agency operations allow for unity of command with a clear hierarchy and established authority.

Unified Command (UC) is an important element in multijurisdictional or multiagency domestic incident management. It provides guidelines to enable agencies with different legal, geographic, and functional responsibilities to coordinate, plan, and interact effectively. UC is designed to be a team effort to overcome much of the

inefficiency and duplication of effort that can occur when agencies from different functional and geographic jurisdictions, or agencies at different levels of government, operate without a common system or organizational framework. All agencies with jurisdictional authority or functional responsibility for any or all aspects of an incident and those able to provide specific resource support participate in the UC structure and contribute to the process of determining overall incident strategies; selecting objectives; ensuring that joint planning for tactical activities is accomplished in accordance with approved incident objectives; ensuring the integration of tactical operations; and approving, committing, and making optimum use of resources. In the case of some multijurisdictional incidents, the designation of a single IC may be considered to promote greater unity of effort and efficiency.[28] Authorities should ensure consent and acknowledgement of participating agencies prior to designating a single IC in multijurisdictional response operations.

Incident Command System (ICS)

The ICS is a widely applicable management system designed to enable effective and efficient incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is a fundamental form of management established in a standard format, with the purpose of enabling incident managers to identify the key concerns associated with the incident, often under urgent conditions. ICS is used to organize on−scene operations for a broad spectrum of emergencies from small to complex incidents, both natural and manmade. The field response level is where emergency management and response personnel, under the command of an appropriate authority, carry out tactical

decisions and activities in direct response to an incident or threat. Resources from the Federal, State, tribal, or local levels, when appropriately deployed, become part of the field ICS as prescribed by the local authority.

As a system, the ICS is extremely useful; not only does it provide an organizational structure for incident management, but it also guides the process for planning, building, and adapting that structure. Using ICS for every incident or scheduled event helps hone and maintain skills needed for the large-scale incidents. Routinely utilizing of a common operational database within the ICS would allow responders the opportunity to provide input to the database and pull information to configure their common operational picture, tailored to the their needs.

ICS is used by all levels of government—Federal, State, tribal, and local—as well as by many private sector and nongovernmental organizations (NGOs). ICS is applicable across disciplines. ICS facilitate activities in five major functional areas: Command, Operations, Planning, Logistics, and Finance/Administration.[29]

## Challenges

### Standards

Component II of the NIMS describes the communications and information management framework necessary for effective emergency management and incident response activities. Incident communications are facilitated through development and use of common communications plans, interoperable communications equipment, processes, standards and architectures. This integrated approach links the operational and support units of the various organizations involved during an incident, which is necessary to maintain communications connectivity and situational awareness.

Planning for communications and information management must address the incident-related policies and equipment, systems, standards, and training necessary to achieve integrated communications.[30] Required characteristics of a common operational picture include interoperability, reliability, scalability, portability, resiliency, and redundancy.[31]

The federal government has mandated the National Incident Management System (NIMS) as a condition of grant funding.[32] While many agencies claim to know and use NIMS, evidence of its field application is weak, especially in relation to multi-agency command from a single incident command post. The reasons for slow or no adoption of NIMS range from traditional resistance to change, to a state of general denial of the possibility that large-scale emergencies can happen in any given jurisdiction, to what may be the biggest factor of all: a reluctance to answer the "who's in charge" question amid historic turf battles, especially those related to police vs. fire department rivalries, and/or squabbles between various levels of government. Cordiality between agencies on the surface can belie the lack of NIMS application in the field.[33]

Exercises should reinforce the use of NIMS and require agencies to demonstrate their proficiency through a certification program. Agencies unable to effectively operate within the NIMS construct should be denied funding and offered training opportunities to meet the mandate. Identifying weaknesses of agencies unable or unwilling to work within NIMS should be accomplished during exercises as opposed to actual incidents when lives may be at stake.

## Interoperability

Interoperability has been used as a catch-all phrase to describe a multitude of issues surrounding emergency scene communications.[34] "Achieving interoperability

requires more than technology. Shifting all the elements requires a comprehensive, coordinated strategy. Interoperability is about technological, strategic, tactical, and cultural change, as much as it is an issue of one radio transmitting to another."[35]

Communications interoperability allows emergency management/response personnel and their affiliated organizations to communicate within and across agencies and jurisdictions. Interoperability is an area of focus as successful emergency management and incident response operations require the continuous flow of critical information among jurisdictions, disciplines, organizations, and agencies.[36]

The time to identify Interoperability issues is during exercises and rehearsals. Work-a-rounds or solutions must be established, tracked, and tested among agencies to ensure requirements are met and a mutually agreeable solution is reached. Technical interoperability issues are usually more easily solved than cultural interoperability issues.

Reliability

Communications and information systems should be designed to be flexible, reliable, and scalable in order to function in any type of incident, regardless of cause, size, location, or complexity. They should be suitable for operations within a single jurisdiction or agency, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement. Communications systems should be applicable and acceptable to users, readily adaptable to new technology, and reliable in the context of any incident to which emergency management/response personnel would be expected to respond.[37]

Emergency responders must have confidence in their equipment and be assured that it will work as advertised when needed.

## Redundancy

The common operational picture and supporting infrastructure must be robust and capable of continued operations in less than optimal conditions. Many different connectivity options exist including conventional wire line service, wireless, and satellite that would provide continued and alternate means of connectivity to a common operational picture either at higher levels of command or at the incident site. The supporting infrastructure must have a Continuity of Operations Plan (COOP) to provide uninterrupted accessibility under all adverse conditions. Alternate and redundant operations sites that can be activated as required are crucial in ensuring continued systems operations and accessibility to provide the information and data necessary for decision makers and incident site commander's situational awareness. Redundant means of connectivity, electrical power, and hardware systems are essential and must be tested and exercised on a routine basis to ensure success.

## Changing Culture

"The desire for a 'turnkey' solution is understandable; the purchase and delivery of new equipment signals tangible evidence that something is being done. Considering that the kind of cataclysmic incidents we are preparing for are infrequent and the statistical exceptions, it is difficult to thoroughly assess the effectiveness of new equipment and procedures, even in the most realistic training exercise environment. Careful insight and informed projections are needed to ensure we do not find ourselves

in the same state of dysfunction ten years from now, because we bought the equipment but did not change our culture and habits."[38]

Organizational culture is engrained in an organization's members and often times the most difficult aspect to change. Biases, past differences, and perceptions must be discarded and a renewed focus on successfully accomplishing objectives established. Organizational leaders must identify cultural differences and issues and work toward a resolution that will alleviate friction and foster a sense of cooperation. Successful unity of effort requires collaboration, coordination, and mutual understanding to attain a common objective.

Recommendations

The following recommendations provide a framework for the successful implementation of a common operational picture process to improve unity of effort in emergency response from the local level through incidents of national significance.

The underlying foundation is a common operational database that serves as a data warehouse with published standards including data architecture, field descriptions, meta-data tags, and clearly defined input and output requirements. The key concept is that data is entered once, properly formatted and tagged, and made available to all that need the information and have the appropriate access permissions. Local responders should populate this data warehouse at the initiation of every response as a standard operating procedure. Establishing this as a routine matter of practice will insure data is captured from the outset and can be used to portray a common operational picture for local responders as well as state and federal agencies should the requirement escalate beyond the capabilities of local authorities.

The common operational picture should be thought of as a process as opposed to a product or “common picture.” Views of the common operational picture could be preconfigured depending on the user and their organizational hierarchy and role, or created on an ad-hoc basis to meet specific requirements. Operational pictures for expected events or scenarios could be pre-designed and stored for use as needed by users with available filters based on location, type of operation, or agency. A user-defined picture allows users at all levels to define their own relevant operational picture displaying the information they require in order to coordinate and manage actions within their area of responsibility and at their operational level.

The Department of Homeland Security, identified as the overall responsible authority by Homeland Security Presidential Directives, should take the lead in bringing organizations together to identify requirements and provide input for the creation of a common operational database possibly using the current HSIN as a baseline. Measures of performance will be essential in determining the effectiveness and efficiency of the system as rated by users and representatives of participating organizations.

DHS should also fund and manage a program for training, support, and maintenance as the identified lead agency for responding to incidents of national significance. Organizations and agencies requesting DHS grants or funding should have to demonstrate their compliance with established standards for use and integration with the common operational database to ensure a unified effort while preventing redundant systems and efforts.

Agencies may continue to use existing applications for displaying operational information or creating their operational picture by reconfiguring their existing systems

to populate and retrieve data from the common operational database ensuring adherence to established data input and output standards.

The initial system should be an unclassified system dealing with Homeland Security emergency responses that do not require classified information sharing between organizations due to the complications a secure system would entail. Homeland Defense requirements involving the need for classified information processing should utilize existing DOD systems operating on the SIPRNET.

## Conclusion

Many local and state emergency response organizations are capable of conducting effective and efficient operations on a small scale where no outside assistance is required. In cases where emergency response requirements overwhelm local and state capabilities, a system is needed to support a common operational picture for decision making and situational awareness at all levels.

Involvement of all levels of government, the private sector, and non-governmental agencies will be required in preventing, preparing for, and responding to incidents of national significance. The NIMS and ICS provide a doctrinal framework and guidelines for emergency response operations. What is needed is a common operational database with standards identifying input and output requirements and an architecture that will allow access based on the users role and organization. With a centralized repository established, data input from all levels can be collected, analyzed, synthesized, and used to populate a user-definable operational picture. This operational picture may be specific to the agency requirement or could be a common picture used by numerous agencies.

Unity of effort in emergency response operations would be greatly enhanced through a user-definable operational picture that can provide information from a common operational database. This system would support decision making, coordination, and integration between emergency response organizations improving efficiency, making better use of resources, and providing a coordinated and timely response during crisis.

The recommendations include changes required to support unity of effort in emergency response and include both technological and cultural change. The most difficult change will involve cultural issues within and between organizations to establish the requirements, standards, and cooperation needed to establish a reliable, redundant, and interoperable system providing data sharing and situational awareness to improve emergency response. This is not a one size fits all solution, but a framework for collecting and storing the pertinent data that organizations require to create and maintain their unique operational picture.

Endnotes

[1] Department of Homeland Security, "National Response Plan," December 2004, 2; available from: http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf; Internet; accessed 29 December 2007.

[2] Department of Homeland Security, "National Incident Management System," Draft August 2007, 24; available from http://www.fema.gov/libraryanser22_nims_report.pdf; Internet; accessed 29 December 2007

[3] Department of Defense Dictionary of Military Terms, available from http://www.dtic.mil/doctrine/jel/doddict/; Internet; accessed 29 December 2007.

[4] Department of Defense, "Chairman of the Joint Chiefs of Staff Instruction 3151.01A Global Command and Control System Common Operational Picture Reporting Requirements;" GL-6; available at www.dtic.mil/cjcs_directives/cdata/unlimit/3151_01.pdf; Internet; accessed 29 December 2007.

[5] James Kievit and John Elliot, "The Sixth Annual USAWC Reserve Component Symposium Achieving Unity of Effort in Responding to Crisis, Workshop # 4: Development and Dissemination of a Common Operational Picture in Preparation, Response, and Recovery Operations," Center for Strategic Leadership Issue Paper Volume 7-07 (August 2007), 3.

[6] Ibid.

[7] Ibid., 4.

[8] George W. Bush, Homeland Security Presidential Directive/HSPD-5, (Washington DC: The White House, 28 February 2003), 1.

[9] Ibid., 3.

[10] Ibid.

[11] Department of Homeland Security, "National Response Plan," December 2004, 2; available from: http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf; Internet; accessed 29 December 2007.

[12] Ibid., 6.

[13] Ibid.

[14] Department of Homeland Security, "National Response Plan II Quick Reference Guide" (Washington DC, May 2006), 2.

[15] Department of Homeland Security, "National Response Plan," (December 2004), 7; available from: http://www.dhs.gov/xlibrary/assets/NRPbaseplan.pdf; Internet; accessed 29 December 2007.

[16] Department of Homeland Security, "National Response Plan II Quick Reference Guide" (Washington DC, May 2006), 2.

[17] Sections 402(a)(1) and 502(a)(1) of the Stafford Act, 42 U.S.C. § 5170(a)(1) and § 5192(a)(1); quoted in National Response Plan, 7.

[18] United States Northern Command Homepage, available from http://www.northcom.mil/ About/index.html ; Internet; accessed 6 January 2008.

[19] Col David H. Gurney (Ret) and Dr. Jeffrey D Smotherman, "An Interview with Victor E. Renuart, Jr, "Joint Force Quarterly Issue 48 (First Quarter 2008): 43.

[20] Bert R. Tussing, "The Sixth Annual USAWC Reserve Component Symposium Achieving Unity of Effort in Responding to Crisis, Workshop # 2: The Potential Need to Establish an Appropriate Mechanism For The Military To Accompany And Support Civilian Components Focused ion Regional Response to Catastrophe," Center for Strategic Leadership Issue Paper Volume 5-07 (August 2007), 4.

[21] Department of Homeland Security Office of the Inspector General, “Homeland Security Information Network Could Support Information Sharing More Effectively,” (Washington, DC), 4-5; available at http://www.washingtonpost.com/wp-srv/nation/documents/OIG_06-38_Jun06.pdf; Internet; accessed 10 January 2008.

[22] Ibid.

[23] Coalition Warrior Interoperability Demonstration Joint Management Office, “Coalition Warrior Interoperability Demonstration 2007 Final Report,” (Hampton/Arlington, VA); available at http://www.cwid.js.mil/public/CWID07FR/htmlfiles/578war.html; Internet; accessed 11 January 2008.

[24] Wikipedia; available at http://en.wikipedia.org; Internet; accessed 13 January 2008.

[25] Department of Defense, “Quadrennial Defense Review,” February 6, 2006; 84; available from http://www.globalsecurity.org/military/library/policy/dod/qdr-2006-report.pdf; Internet; accessed 29 December 2007.

[26] Department of Homeland Security, “National Incident Management System,“ Draft August 2007; available from http://www.fema.gov/libraryanser22_nims_report.pdf; Internet; accessed 29 December 2007.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] U.S. Department of Homeland Security, “Jurisdictions will be required to meet the FY 2006 NIMS implementation requirements as a condition of receiving federal preparedness funding assistance in FY 2007.”, The NIMS Integration Center, National Standard Curriculum Training Development Guidance (Washington, D.C., 2005).

[33] Ronald P. Timmons, *Interoperability: Stop Blaming the Radio*; Homeland Security Affairs, Volume III, No 1 (February 2007), 8-9.

[34] Ibid., 1.

[35] U.S. Department of Defense, “DOD Instruction Number 4630.8”, June 30, 2004, Section E2.1.32, 53; available from http://jitc.fhu.disa.mil/jitc_dri/pdfs/i46308.pdf; Internet; accessed 31 December 2007.

[36] Department of Homeland Security, “National Incident Management System,“ Draft August 2007; 24; available from http://www.fema.gov/libraryanser22_nims_report.pdf ; Internet; accessed 29 December 2007.

[37] Ibid.

[38] Timmons, 3.